ENJOY SAFER TECHNOLOGY™

ESET THREAT INTELLIGENCE

Extienda su inteligencia de seguridad desde la red local hasta el espacio cibernético global

Los ataques dirigidos, las amenazas persistentes avanzadas (APT), las actividades *0-day* y las actividades de las botnets, son difíciles de detectar cuando solo se cuenta con la información de la propia red corporativa. Para evitarlo, es imprescindible que las empresas cuenten con una inteligencia más profunda y una protección eficiente.

ESET Threat Intelligence elimina la brecha entre la información de seguridad cibernética que se recibe de la propia red corporativa y la inteligencia en el espacio cibernético que ESET recopila en todo el mundo. Utiliza la información proveniente de más de 100 millones de sensores y la envía a ESET a través de ESET LiveGrid®, el sistema en la nube de protección contra malware. Dicha información se canaliza a través de los múltiples centros de investigación y desarrollo de ESET en todo el mundo, que se dedican exclusivamente a la seguridad cibernética y que proporcionan a sus clientes un conocimiento único, para ayudarlos a entender y gestionar el riesgo empresarial y convertir las amenazas desconocidas en conocidas y mitigadas, mejorando la efectividad de sus defensas.

Suministro de datos en tiempo real y API

El sistema de suministro de datos de ESET Threat Intelligence emplea el formato ampliamente utilizado STIX/TAXII para intercambiar información sobre la inteligencia de amenazas. Facilita la integración con la herramienta existente SIEM de los proveedores de servicios de seguridad y permite obtener la información más reciente sobre el panorama de amenazas (especialmente las botnets). De esta forma, ayuda a predecir y prevenir las amenazas, incluso antes de que efectúen sus ataques, y fortalece la seguridad de los clientes finales por adelantado. Además, está disponible la API de ESET Threat Intelligence para automatizar la generación de informes, las reglas Yara y otras funcionalidades desde cualquier otro sistema que utilice el cliente.

Protección contra malware

El sistema en la nube de protección contra malware provisto por ESET es una de las muchas tecnologías basadas en ESET LiveGrid®, nuestro sistema en la nube. Las posibles amenazas son monitoreadas y enviadas a la nube de ESET a través del sistema de recopilación de datos ESET LiveGrid, donde automáticamente se ponen en un modo de sandbox y se analiza su comportamiento.

*Las aplicaciones desconocidas sospechosas y las potenciales amenazas se monitorean y se envían a la nube de ESET a través del **sistema de recopilación de datos, ESET LiveGrid.***

*Las muestras recopiladas se **verifican automáticamente en el modo sandbox** y se someten al análisis de su comportamiento. Si se confirma su caracter malicioso, se crean nuevas firmas de detección automatizadas.*

*Los clientes de ESET reciben las nuevas detecciones automatizadas a través del **sistema de reputación de archivos ESET LiveGrid** , sin necesidad de esperar a la próxima actualización de la base de firmas.*

Reputación y caché

Al analizar un archivo o una URL, nuestras soluciones primero comprueban la memoria caché local para ver si se trata de objetos conocidos, ya sean maliciosos o no (incluidos en la lista blanca), mejorando el rendimiento de la exploración. A continuación, la reputación del objeto se busca en nuestro sistema de reputación de archivos ESET LiveGrid®.

ESET LiveGrid recopila información relacionada a amenazas proveniente de millones de usuarios de ESET para determinar la edad del archivo y su prevalencia.

La amenazas desconocidas, se envían a ESET para continuar con su análisis y procesamiento.

La lógica de nuestro servidor en la nube evalúa estos datos en forma automática y suministra una respuesta rápida a través de las listas blancas y negras.

Informe de malware dirigido

Nuestro informe mantiene informado al usuario sobre los ataques potenciales y en curso dirigidos específicamente contra su organización. Las reglas personalizadas se pueden configurar usando Yara para obtener la información específica de la empresa en la que estén interesados los ingenieros de seguridad. Gracias a este informe, el usuario obtiene detalles valiosos sobre las campañas de malware en curso o potenciales, incluyendo la cantidad de veces que se detectaron en todo el mundo, las direcciones URL que contienen códigos maliciosos, el comportamiento malicioso en el sistema, la ubicación, entre otros datos.

Informe sobre actividad de botnets

Brinda informes periódicos y datos cuantitativos sobre las familias de malware identificadas y las variantes de tipo botnet. El informe suministra una lista de los servidores de comando y control conocidos (C&C) que participan en la administración de las botnets, así como una lista de los objetivos del malware. Las listas se clasifican por tipo de malware.

Análisis automatizado de muestras

Cuanto uno más sabe, es menos crédulo. Este informe personalizado basado en el archivo o *hash* enviado brinda información valiosa para la toma de decisiones basadas en hechos y en la investigación de incidentes.

Seguridad adicional

Los analistas de seguridad recomiendan el uso de enfoques diferentes con el fin de minimizar las potenciales debilidades que pueden surgir cuando se usa una solución de seguridad de un solo proveedor.

ESET Threat Intelligence no requiere que las soluciones para endpoints o servidores de ESET estén instaladas en la red del usuario. De esta manera, puede ser utilizado por clientes que no son de ESET como capa adicional de seguridad para ayudar a alertarlos de campañas de malware inminentes o de amenazas específicas sobre las que su proveedor de seguridad actual puede no estar al corriente.

Detecciones por ADN

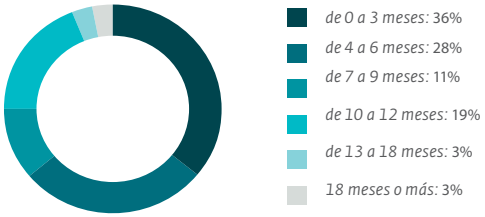
Las detecciones de ADN son definiciones complejas de comportamiento malicioso y características de malware. Aunque el código malicioso puede ser fácilmente modificado u ofuscado, el comportamiento del objeto no se puede cambiar con tanta facilidad. Por eso, la detección del ADN es capaz de identificar el malware nunca antes visto que contiene genes que indican un comportamiento malicioso.

*La **heurística avanzada** detecta proactivamente el malware desconocido.*

***Detecta el malware según su funcionalidad** mediante el análisis de su comportamiento.*

*Las **técnicas avanzadas**, como la exploración basada en ADN, identifican las amenazas según la estructura de su código.*

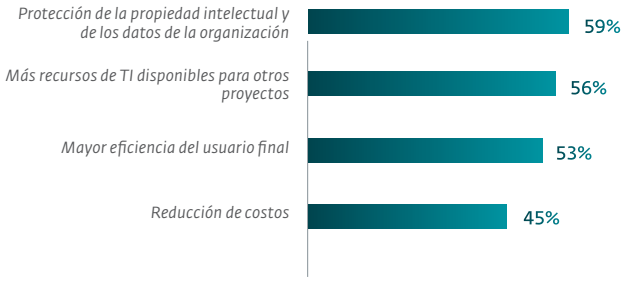
El 64% de los clientes de ESET notan un retorno de su inversión en menos de 6 meses, y el 75% dentro de los 9 meses.



TechValidate by SurveyMonkey

Encuesta de TechValidate a 552 usuarios de ESET Security Solutions que respondieron la siguiente pregunta: "¿En cuánto tiempo estima que notó un retorno de su inversión con las soluciones de seguridad de ESET?" Fuente > https://www.techvalidate.com/product-research/eset-security-solutions/charts/3DB-C32-72B

¿Cuáles son los beneficios operativos que notó al implementar las soluciones de seguridad de ESET?



TechValidate by SurveyMonkey

Encuesta de TechValidate a 1.213 usuarios de ESET Security Solutions. Fuente > https://www.techvalidate.com/product-research/eset-security-solutions/charts/159-B6C-752

AV comparatives ADVANCED+ HEURISTIC / BEHAVIOURAL TEST MAR 2015

ESET recibió la mayor cantidad de premios "Advanced+" en las Pruebas proactivas de AV-Comparatives.

AV comparatives ADVANCED+ REAL WORLD PROTECTION TEST DEC 2015

ESET recibió el premio "Advanced+" en la Prueba de protección en el mundo real, llevada a cabo por AV-Comparatives.

vb VERIFIED SPAM virusbtn.com

ESET obtuvo la mayor cantidad de premios VB100 consecutivos por detección de malware entre todos los proveedores de seguridad informática. Ha obtenido excelentes resultados en todas las pruebas VB100 desde el año 2003.

vb March 2016 VERIFIED SPAM + virusbtn.com

ESET tiene el mejor puntaje por su detección de spam, otorgado por Virus Bulletin.

eset ENJOY SAFER TECHNOLOGY™

Acerca de ESET: Desde 1987, ESET® desarrolla multipremiadas soluciones de seguridad que ayudan a más de 100 millones de usuarios a disfrutar de la tecnología en forma más segura. Su amplia cartera de productos de seguridad protege todas las plataformas populares, y ofrece un equilibrio perfecto entre rendimiento y protección proactiva para empresas y consumidores de todo el mundo. La empresa cuenta con una red global de ventas que abarca más de 180 países, y oficinas regionales en Bratislava, San Diego, Singapur y Buenos Aires. www.eset-la.com